AF

PTO/SB/21

U.S. Department of Commerce
Patent and Trademark Office
PATENT

AMENDMENT TRANSMITTAL FORM

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Customer No.: 23696
Attorney Docket No.: 010001
In Re Application of: Anthony Mauro
Serial Number: 09/826,742
Filed: April 5, 2001
Examiner: Courtney Fields
Group Art Unit: 2137

Dear Sir:

Transmitted herewith for filing is an APPEAL BRIEF UNDER 37 CFR §41.37 in the above identified application.

CLAIMS	(a) Number Remaining After Amendment	(b) Highest Number Previously Paid For	(c) Extra Claims	Large Entity Fee	Fee Paid
Total*	26	26	0	x $50 =	$0
Independent**	4	4	0	x $200 =	$0
Multiple Dependent Claim(s): □ Yes ☒ No				$360	$
EXTENSION FEES			□ One Month	$120	$
			□ Two Months	$450	$
			□ Three Months	$1020	$
TERMINAL DISCLAIMER				$130	$
				TOTAL FEE	$0

*If the number in column a is less than 20, enter 0 in column c.
**If the number in column a is less than 3, enter 0 in column c.

4. □ Fee check in the amount of $_____ is enclosed to pay for any claim and/or extension fees.
5. □ Please charge Deposit Account No. 17-0026 of QUALCOMM Incorporated the amount of $_____. The Commissioner is hereby authorized to charge payment of any additional fees that may be required, or credit any overpayment to said Deposit Account No. 17-0026. A duplicate of this sheet is enclosed for fee processing.
6. ☒ The Commissioner is further hereby authorized to charge to said Deposit Account No. 17-0026, pursuant to 37 CFR 1.25(b), any fee whatsoever which may become properly due or payable, as set forth in 37 CFR 1.16 to 37 CFR 1.18 inclusive, for the entire pendency of this application without specific additional authorization.

Date: December 7, 2005

Signature: Richard A. Bachand
Richard A. Bachand, Reg. No. 25,107
Phone No. (858) 845-8503

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Telephone: (858) 658-5787
Facsimile: (858) 658-2502

CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.8(a))

I hereby certify that this correspondence is, on the date shown below, being:

MAILING

☒ deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Depositor's Name: Victoria J. Pacey
(type or print name)

Date: December 7, 2005

FACSIMILE

□ transmitted by facsimile to the Patent and Trademark Office.

Depositor's Name:
(type or print name)

Signature: ______________________

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:
Anthony Mauro

Serial No.: 09/826,742

Filed: April 5, 2001

For: METHOD AND APPARATUS FOR PROVIDING SECURE PROCESSING AND DATA STORAGE FOR A WIRELESS COMMUNICATION DEVICE

Group Art Unit: 2137

APPEAL BRIEF UNDER 37 CFR §41.37

MAIL STOP: Appeal Brief - Patents
Asst. Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313

Attention: Courtney Fields
Examiner

Appellant offers this Brief in furtherance to the Notice of Appeal mailed October 17, 2005.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to the Commissioner of Patents and Trademarks, Alexandria, VA 22313, on:

December 7, 2005
(Date of Deposit)

Victoria J. Pacey
(Name of Person Making Deposit)

(Signature)

I. REAL PARTY IN INTEREST:

At the time of the filing of this appeal brief, Qualcomm Corporation is the real party in interest for this appeal.

II. RELATED APPEALS AND INTERFERENCES:

No other appeals or interferences are known which will directly affect, are directly affected by, or have a bearing on the board decision of the pending appeal.

III. STATUS OF CLAIMS:

Claims 1-26 are currently pending in the application, but stand rejected by the Examiner. Claims 1-26 were originally filed in the application on April 5, 2001.

Claims 1-26 are believed improperly rejected and are the subject of this appeal. A copy of the claims as rejected is attached as an Appendix.

IV. STATUS OF AMENDMENTS:

All Amendments have been entered. In response to a first Office Action ("Office Action") dated September 23, 2004, an Amendment was filed on March 15, 2005. A Final Office Action ("Final Office Action") was mailed June 3, 2005, and a Notice of Appeal was filed on October 17, 2005 in response to that Final Office Action.

This Appeal Brief is filed in response to the Final Office Action mailed on June 3, 2005. No Amendments are un-entered.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER:

Techniques are described for providing secure processing and data storage for a wireless communication device. In one embodiment, a remote terminal **110** includes a data processing unit **210**, a main processor **230**, and a secure unit **240** (Original Application, p. 4, l. 30 - p. 7, l. 9; Fig. 2). The data processing unit processes data for a communication over a wireless link. The main processor provides control for the remote terminal. The secure unit **240** includes a secure processor **250** that performs the secure processing for the remote terminal **110** (e.g., using public-key cryptography) and a memory **254** that provides secure storage of data (Id., p. 6, l. 30 - p. 8, l. 17; Fig. 3).

In another embodiment, the secure processor and memory may be implemented within a single integrated circuit (Id., p. 7, l. 17 - l. 21). The single integrated circuit includes a data processing unit **210**, a main processor **230**, and a secure unit **240** embedded within the main processor (Id.).

In another embodiment, a method for performing secure processing within a communication device is defined. The method recites defining a secure processor **250** and secure storage **254** within the communication device for performing secure processing with hardcoded protocols (Id., p. 6, l. 30 - p. 7, l. 4; Fig. 3). The secure processor and secure storage are physically encapsulated within a secure unit (Id., p. 7, ll. 5-8).

Another embodiment describes a method for providing secure processing and data storage for a wireless communication device. A first message to initiate a secure transaction with a foreign entity is received (Id., p. 8, ll. 18-33). The foreign entity is authenticated (Id., p. 9, ll. 7-8). Securing processing for the transaction is performed through the secure unit which is physically encapsulated within a secure module (Id., p. 7, ll. 5-8).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL:

Claims 1-11 and 20-23 stand rejected as anticipated by the cited portions of U.S. Patent No. 6,026,293 to Osborn (hereinafter "Osborn"). Sections 1 and 2 of the Office Action, mailed June 3, 2005, describe the Examiner's current position on this issue.

Claims 12-19 and 24-26 stand rejected as obvious over Osborn in view of the cited portions of U.S. Patent No. 5,987,140 to Rowney et al. (hereinafter "Rowney"). Sections 3 and 4 of the Office Action, mailed June 3, 2005, describe the Examiner's current position on this issue.

VII. ARGUMENT:

I. 35 U.S.C. §102(e) Rejection of Claims 1-19

Claims 1-11 are rejected under 35 U.S.C. §102(e) as being anticipated by Osborn. Claims 12-19 each depend from independent claim 1, and these claims are also rejected under Osborn using the same rationale as found in claims 1-11. The Appellant believes that the rejection is flawed for the reasons that follow.

For fundamental teaching on the doctrine of anticipation, one must consider the decision of Judge Rich in *In re* William J. King, 801 F.2d 1324, 231 U.S.P.Q. 136 (Fed. Cir. 1986):

> It is axiomatic that anticipation of a claim under §102 can be found only if the prior art reference discloses every element of the claim, and that anticipation is a fact question subject to review under the clearly erroneous standard. Our review of a finding of anticipation is the same whether it was made by the board or by a district court. (citations omitted)
>
> *In re* William J. King, 801 F.2nd at 1326 (emphasis added).

Further, for a reference to anticipate a claim under 35 U.S.C. §102, that reference must teach, or identically describe, each and every element or step of the claim. See, e.g., Jamesbury Corp. v. Litton Industrial Products, 756 F.2d 1556, 225 USPQ 253 (Fed. Cir. 1985). "Anticipation" is a restrictive concept, requiring the presence in a single prior art disclosure of each and every element of a claimed invention. Further, "there must be no difference between the claimed invention and the reference disclosure, as viewed by a person of ordinary skill in the field of the invention." (emphasis added, Scripps Clinic & Research Foundation v. Genentech, Inc., 927 F.2d 1565, U.S.P.Q.2d 1896 (Fed. Cir. 1991)). As discussed below, the Osborn patent does not disclose the identical structure and methods described in the claims of the present application.

Referring to independent claim 1, the Examiner cites wide portions of Osborn as anticipating all elements of this claim (Final Office Action, p. 3, sec. 2, *citing* Osborn, col. 7, ll. 60-67; col. 8, ll. 1-62). However, these portions of Osborn simply describe a processor and various memory contents, wherein an "audit" hash value derived from memory contents is compared to an "authenticated" or "valid" hash value derived from authentic memory contents to determine whether tampering has occurred with the memory (Osborn, col. 8, ll. 30-42).

Notably, Osborn does *not* describe "a secure unit operatively coupled to the main processor," as claimed in claim 1. The secure unit of claim 1 of the application includes "a secure processor" and "a secure memory." Osborn's cellular telephone has no such "secure unit," as it simply describes multiple unsecured components of a conventional cellular telephone.

Fig. 4 of Osborn illustrates how a "controller 400 communicates with the flash program memory 420, the RAM 408 and the EEPROM 410 via memory bus 424" (Osborn, col. 8, ll. 16-18). "The EEPROM 410 includes user profile data 412 ... and a signed/unsigned valid hash value pair 419." (Id., col. 8., ll. 6-8). It is not suggested that these components are secured, and thus they simply do not comprise a *secure unit.* Moreover, on the cellular phone of Osborn, there is merely a single microprocessor, not the main processor and secure processor found in claim 1.

Referring to Fig. 5 of Osborn, after the cellular telephone is turned on and the controller 400 is initialized, hash code from the controller "is then run to perform an audit hash value calculation over selected contents ... stored in EEPROM 410" (Id., col. 8, ll. 21-27). After this:

> [t]he controller then authenticates the signed valid hash value pair 418 stored in the EEPROM 410 .... The authenticated hash value is then stored in PSRAM 407 (block 506). The audit hash value ... is then compared with the authenticated hash value derived at block 504 (block 508). If the two hash values match, a microprocessor program counter is set to an appropriate location in the flash memory 420, and a periodic hash value calculation process is enabled (block 510), whereafter the cellular telephone begins normal operation (block 512). If the hash values do not match at block 508, the system is put into an infinite loop (block 514), or is otherwise disabled.

(Id., col. 8, ll. 28-42). This text simply discusses multiple unsecured components of a conventional cellular telephone working in conjunction over a shared bus. These unsecured components carry out a **comparison** between an audit and an authentic hash value in order to detect whether tampering has occurred with the flash memory or the EEPROM. If so, they merely render the telephone operable or inoperable according to the outcome of the comparison (see, e.g., Osborn, col. 8, ll. 45-46). It does not secure the telephone from tampering in the first place - instead, it determines whether a telephone has already been tampered with. This teaching of Osborn does not provide secure processing or secure data storage. The components in this part of the Osborn patent (e.g., the EEPROM 410, controller 400, flash program memory 420) do *not* comprise "a secure unit operatively coupled to the main processor," as claimed in claim 1.

In the Final Office Action, the Examiner asserts in his *Response to Arguments* section that Figure 12 shows the secure processor and secure unit described in the Claim 1 (Final Office Action, p. 2, *Response to Arguments* sec. 3). However, this "secure processor" in Osborn is in fact a ***separate*** data transfer device (Osborn, col. 10, ll. 8-10). In this second part of Osborn, the ***separate*** data transfer device is authenticated with an authentication process before being allowed to perform data transfer from the separate device to the cell phone. Figure 12 then illustrates an example of how the device may be used to reprogram the cellular phone of Osborn.

There are, thus, two distinct portions of Osborn which are cited by the Examiner. One performs testing on the memory of the phone ("memory validation") to determine whether it has been tampered with. These components of the Osborn patent, which perform the comparison between the audit and valid hash values, are clearly not "physically encapsulated within a secure module and further configured to *prevent* unauthorized access to the secure memory via hard-coded protocols," as set forth in claim 1 of the application (emphasis added).

The other aspect of Osborn involves a *second* data transfer device which is separate from the cellular phone, and which may be connected with the phone by connector, and then authenticated. Even if the secure processor of this second device was deemed part of the cellular phone (and this is not suggested or implied), there is no teaching in Osborn that this secure processor be "physically encapsulated" in a "secure module." Moreover, Osborn fails to teach that the secure unit be configured to prevent unauthorized accesses to the secure memory via "hardcoded protocols."

The elements of independent claim 1 of the application are not disclosed in Osborn. The cited art, therefore, does not support the rejection of claims 1. As Osborn does not anticipate independent claim 1, Osborn cannot anticipate claims 2-19 which each depend from claim 1. The rejection of claims 2-19 is, therefore, unsupported by the cited art.

II. 35 U.S.C. §102(e) Rejection of Claim 20

Referring to independent claim 20, the Examiner cites specific portions of Osborn as anticipating all elements of this claim (Final Office Action, p. 3, sec. 2, *citing* Osborn, col. 7, ll. 60-67; col. 8, ll. 1-62). However, as noted above, these portions of Osborn simply describe a microprocessor 400 and various memory contents, wherein an "audit" hash value derived from memory contents is compared to an "authenticated" or "valid" hash value derived from authentic memory contents to determine whether tampering has occurred with the memory (Osborn, col. 8, ll. 30-42). Osborn does *not* describe "a secure unit embedded within the main processor," as claimed in claim 20 of the application.

These cited portions of Osborn simply discuss multiple unsecured components of a conventional cellular telephone communicating over a shared bus. The components carry out a comparison between an audit and an authentic hash value in order to detect tampering, and render the telephone operable or inoperable according to the outcome of the comparison. Notably, Osborn does not necessarily secure the telephone from tampering in the first place. The microprocessor of Osborn does not provide secure processing. The microprocessor and memory components in the Osborn patent do *not* comprise "a secure unit embedded within the main processor," as claimed in claim 20 of the application.

Additionally, it is clear from the foregoing that those components of the Osborn patent which perform the comparison between the audit and valid hash values clearly do not comprise a secure unit "configured to *prevent* unauthorized accesses to securely stored data via hard-coded protocols," as set forth in claim 20 of the application (emphasis added).

In the Final Office Action, the Examiner asserts in his Response to Arguments section that Figure 12 shows a secure unit serving as "secure data storage for secure processing for a cellular telephone" (Final Office Action, p. 2, *Response to Arguments*, sec. 3). However, as noted above, this "secure processor" in Osborn is in fact a ***separate*** data transfer device (Osborn, col. 10, ll. 8-10). As a ***separate*** device, it is thus clear that it cannot comprise "a secure unit embedded within the main processor," as called for in claim 20. Nor does it prevent unauthorized accesses to securely stored data via hard-coded protocols.

III. 35 U.S.C. §102(e) Rejection of Claims 21-23

Regarding independent method claim 21, the Examiner cites additional portions of Osborn as anticipating all elements of the claim (Final Office Action, *citing* Osborn col. 3, ll. 61-67, col. 4, ll. 1-8, col. 8, ll. 19-62, and col. 9, ll. 30-62). But these portions of Osborn do not describe the elements of claim 21. The cited portions of columns 3 and 4 of Osborn pertain to Fig. 3, which is described as a prior art "conventional cellular telephone memory and processor arrangement" (Osborn, col. 3, 11. 62-63). Columns 8 and 9 of Osborn describe the comparison between the audit and valid hash values described above.

And for the same reasons as noted above, these components do not define "a secure processor within the communications device" for performing secure processing, or define "secure storage within the communication device " for providing secure data storage. Nor is there any description of storing "hardcoded protocols" for secure processing, or of "physically encapsulating the secure processor and secure storage within a secure unit," as provided in claim 21. Instead, the unsecured components of Osborn merely render the telephone inoperable if the comparison fails. The audit hash value calculation may be performed periodically, but it is simply a comparison performed by the conventional components of a cellular telephone which then renders the telephone operable or inoperable.

Elements of independent claim 21 of the application are not disclosed in Osborn, and the rejection of claim 21 is therefore not supported and should be withdrawn. As Osborn does not anticipate independent claim 21, Osborn cannot anticipate dependent claims 22-23 depending from claim 21, and should be withdrawn as well.

IV. 35 U.S.C. §103(a) Rejection of Claims 12-19

The Examiner rejected claims 12-19 under 35 U.S.C. §103(a) as unpatentable over Osborn in view of Rowney. The rejections are respectfully traversed. The Appellant submits that the differences between the subject matter sought to be patented, and the references cited by the Examiner, are not such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains.

The patent office is charged with putting forth a *prima facie* showing of obviousness. The Appellant believes a *prima facie* case of obviousness has not been properly set forth in the Final Office Action. As succinctly stated in the MPEP:

> "To establish a *prima facie* case of obviousness, ... there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. [Also] the prior art reference (or references when combined) must teach or suggest all the claim limitations." See MPEP §2143.

Missing Limitations: Claims 12-19 depend directly or indirectly from independent claim 1. All claim limitations of the rejected claims 12-19 must be considered, especially when one or more are missing from the cited prior art. Applicant's arguments, *supra*, regarding claim 1, clearly show that Osborn does teach or suggest the limitations of claim 1, and the arguments are not repeated here.

Motivation to Combine: A *prima facie* showing requires that the "teaching or suggestion to make the claimed combination . . . must . . . be found in the prior art, not in the applicant's disclosure." MPEP §2143. In rejecting dependent claims 12-19, the Office has not put forward any motivation to combine the teachings of Rowney and Osborn to teach the limitations of the claims.

The Rowney patent describes secure data transmission between computer systems over a public communication system such as the Internet. The Examiner cites Rowney for discussing one or more security protocols, for action in a client or server role, for the storage of electronic farads, for the storage of cryptographic parameters, and for the storage of authentication certificates. Rowney does not teach use of the security protocols with a remote terminal in a wireless communication system as set forth in claim 1 of the application. There is no cited teaching or suggestion to combine the teachings of Rowney with Osborn

It is well established that "[i]t is impermissible to use the claimed invention as an instruction manual or 'template' to piece together the teachings of the prior art so that the claimed invention is rendered obvious." *In re* Fritch, 23 U.S.P.Q.2d 1780, 1784 (Fed. Cir. 1992). That is, however, what the Examiner has done in this case.

The obviousness rejections of claims 12-19 by the Examiner are unsupported by the cited art.

V. 35 U.S.C. §103(a) Rejection of Claims 24-26

The Examiner rejected claims 24-26 under 35 U.S.C. §103(a) as unpatentable over Osborn in view of Rowney. Referring to independent claim 24, the Examiner cites new portions of Rowney to teach the limitations (Final Office Action, p. 7, *citing* Rowney col. 10, ll. 31-67 and col. 11, ll. 1-44). The Appellant again asserts that no *prima facie* showing has been put forward.

Missing Limitations: The cited portions of Rowney discuss the process between a customer computer system and a merchant computer system (see Rowney, Fig. 2) for initiating communication (via "hello" procedure), verifying each computer's identity, and exchanging a decryption key. Again, there is no teaching or suggestion in either Osborn or Rowney of a "secure unit physically encapsulated within a secure module" of a wireless communication device as set forth in claim 24 of the application. Applicant again refers to the arguments, *supra,* regarding Osborn with respect to claims 1 and 20. Rowney fails to teach or suggest the secure unit physically encapsulated within a secure module for a wireless communication device. The obviousness rejections of claims 24-26 by the Examiner are unsupported by the cited art and should be withdrawn.

Motivation to Combine: As noted above, the "teaching or suggestion to make the claimed combination ... must ... be found in the prior art, not in the applicant's disclosure." MPEP §2143. In rejecting dependent claims 24-26, the Office at best relies upon the contention that the references, when combined, offer benefits. Unless the art itself "suggests the desirability of the combination," benefits alone are not enough. MPEP §2143.1.

The obviousness rejections of claims 24-26 by the Examiner are unsupported by the cited art.

CONCLUSION

In light of the foregoing, it is clear that claims 1-26 are allowable. The Appellants therefore respectfully request that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

Dated: December 7, 2005

By: Richard A Bachand
Richard A. Bachand
Attorney for Applicant
Registration No. 25,107

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121-2779
Telephone: (858) 845-8503
Facsimile: (858) 658-2502

60626400 v1

APPENDIX LIST OF PENDING CLAIMS

1. (Original) A remote terminal in a wireless communication system, comprising:

a data processing unit configured to process data for a communication over a wireless link;

a main processor coupled to the data processing unit and configured to provide control for the remote terminal, wherein the data processing unit and main processor are unsecured units vulnerable to being spoofed by external entities; and

a secure unit operatively coupled to the main processor and including

a secure processor configured to perform secure processing for the remote terminal, and

a secure memory configured to provide secure storage of data, and

wherein the secure unit is physically encapsulated within a secure module and further configured to prevents unauthorized accesses to the secure memory via hardcoded protocols.

2. (Original) The remote terminal of claim 1, wherein the secure unit further includes

a read only memory (ROM) configured to store program instructions and parameters used for the secure processing.

3. (Original) The remote terminal of claim 2, wherein the ROM is embedded within the secure processor.

4. (Original) The remote terminal of claim 1, wherein the secure processor and secure memory are implemented and physically encapsulated within a single integrated circuit (IC).

5. (Original) The remote terminal of claim 1, wherein the secure processor and secure memory are physically encapsulated within a tamper resistance or tamper evident unit.

6. (Original) The remote terminal of claim 1, wherein the secure processor and secure memory are permanently affixed within the remote terminal.

7. (Original) The remote terminal of claim 1, wherein messaging and data are exchanged with the secure unit via a single entry point provided by a bus.

8. (Original) The remote terminal of claim 1, wherein the secure unit is configured to implement public-key cryptography for the secure processing.

9. (Original) The remote terminal of claim 8, wherein a private key assigned to the remote terminal is embedded within the secure processor.

10. (Original) The remote terminal of claim 9, wherein the private key is permanently etched within the secure processor.

11. (Original) The remote terminal of claim 9, wherein the private key assigned to the remote terminal is stored in a ROM within the secure processor.

12. (Original) The remote terminal of claim 1, wherein the secure processor is configurable to implement one or more security protocols.

13. (Original) The remote terminal of claim 12, wherein the one or more security protocols include Secure Sockets Layer (SSL) protocol or Transport Layer Security (TLS) protocol, or both.

14. (Original) The remote terminal of claim 1, wherein the secure unit is configurable to act in a role of a client or a server for each secure transaction with a foreign entity.

15. (Original) The remote terminal of claim 1, wherein the secure memory is configured to store electronics funds.

16. (Original) The remote terminal of claim 1, wherein the secure memory is configured to store cryptographic parameters used for the secure processing.

17. (Original) The remote terminal of claim 1, wherein the secure memory is configured to store one or more certificates used for authentication.

18. (Original) The remote terminal of claim 17, wherein a certificate is loaded into the secure memory via a secure transaction with a certificate authority.

19. (Original) The remote terminal of claim 18, wherein different levels of security is implemented for a certificate loading transaction depending on whether or not a certificate has already been loaded to the remote terminal.

20. (Original) A remote terminal in a wireless communication system, comprising:

a data processing unit configured to process data for a communication over a wireless link;

a main processor coupled to the data processing unit and configured to provide control for the remote terminal, wherein the data processing unit and main processor are unsecured units vulnerable to being spoofed by external entities; and

a secure unit embedded within the main processor and configured to perform secure processing for the remote terminal and provide secure storage of data, wherein the secure unit is further configured to implement public-key cryptography for the secure processing, and wherein the secure unit is further configured to prevents unauthorized accesses to securely stored data via hardcoded protocols.

21. (Original) A method for providing secure processing and data storage for a wireless communication device, comprising:

defining a secure processor within the communication device for performing secure processing;

defining a secure storage within the communication device for providing secure data storage;

storing program instructions and parameters used for the secure processing within the secure processor or secure storage, wherein the stored program instructions implement hardcoded protocols; and

physically encapsulating the secure processor and secure storage within a secure unit.

22. (Original) The method of claim 21, wherein the secure processor and secure storage are physically encapsulated within a single integrated circuit (IC).

23. (Original) The method of claim 21, further comprising:

permanently affixing the encapsulated secure processor and secure storage within the communication device.

24. (Original) A method for providing secure processing and data storage for a wireless communication device, comprising:

receiving a first message to initiate a secure transaction with a foreign entity;

authenticating the foreign entity through a secure processor located within the communication device; and

if the foreign entity is authenticated, performing securing processing for the secure transaction through the secure processor, and

wherein the secure unit is physically encapsulated within a secure module and further configured to prevents unauthorized accesses to the secure memory via hardcoded protocols.

25. (Original) The method of claim 24, wherein the secure processing is performed based on program instructions stored within the secure processor.

26. (Original) The method of claim 24, wherein the authentication is achieved via exchanges of certificates.